Effective Date: 11/15/2017

Appropriate Use of Software Standard

Purpose

The Appropriate Use of Software Standard is intended to facilitate compliance with the listed policies/standards and associated Information Technology (IT) Security Policy objectives:

- Configuration Management Policy and Standard
- Maintenance Policy and Standard
- Media Protection Policy and Standard
- System and Information Integrity Standard
- System and Service Acquisition Policy and Standard

Standard

DET/State systems and system environments must utilize (purchase, install, and/or access) only approved, State-owned, and State-licensed software on DET/State systems and system environments (CM-10, CM-11, SA-5).

All approved, state-owned and licensed software and associated documentation must be utilized in accordance with the terms and conditions of contract agreements (including End-User License Agreements, ELUA), copyright laws, and state/federal laws (SA-5).

In addition, DOA/DET is required to:

- Ensure demonstrations of pre-purchased (evaluation) software are conducted in a secure, non-production environment (SA-2, SI-7);
- Track the use of software and associated documentation protected by quantity licenses to control copying and distribution (CM-10, SI-7);
- Control and document the use of peer-to-peer file sharing technology and other file sharing technologies (i.e. file shares) to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work (CM-10);
- Audit (e.g. software vendor audit), remove, destroy, or uninstall software in a timely manner in accordance with contractual agreement and copyright laws (MP-4, MP-6, SI-7); and,
- Allow only authorized and trained technicians to (can) install software (MA-5).

Software use requirements for individuals using DET/State Systems (including agency-issued mobile devices), environments, and information include:

- Use of only approved, state-owned, and state-licensed software on DET/State systems and system environments (CM10, CM-11);

Effective Date: 11/15/2017

- Individuals cannot enter in to an agreement/contract (includes click-thru agreements) for software use on DET/State systems and system environments (CM-10, CM-11, SI-7); and,
- Individuals cannot install unregistered or unauthorized software (including unlicensed, demo, and/or personally-owned software) on DET/State systems and system environments (CM-10, CM-11, SI-7).

Definitions

- Agency - State of Wisconsin legislatively defined Departments and all customers of DET services, equipment, and/or technologies.
- DET/State information - Any information that is created, accessed, used, stored, or transmitted by an Agency and/or DET.
- DET/State information systems and system environments - All equipment or services used to input, store, process, transmit, and output information, including, but not limited to: network devices, servers, databases, printers, Internet, email, physical, virtual, cloud, and applications accessible to and/or managed by DET.

Compliance References

IRS Pub. 1075
NIST 800-53 Revision 4

Exception Process

Exceptions to this and all DET Security policies or procedures must follow the DET Exception Procedure.

Document History/Owner

This standard was developed as required by the Department of Administration, DET Information Technology Security Policy Handbook, under the authority of Wisconsin State Statute 16.971.

This standard is effective upon approval and publication until retired. Revisions and updates continue the effective date by documenting required changes over time.

Ownership for this standard is assigned to the DET Bureau of Security. As such, the DET Bureau of Security is responsible for the maintenance, update(s), and review of this document annually before the anniversary of the effective date.

Effective Date: 11/15/2017

Version	Approval/Revision/ Review Date	Description	Approver/Author, Title
.1	7/25/2016	Original	Tanya Choice Cybersecurity Compliance Consultant
.2	9/29/2016	Approved final draft	J. Thompson, B. Farrar, T. Choice, E. Ford, K. Skiera
1.0	11/6/2017	Final approval	Bill Nash, CISO

Authorized and Approved by:

Bill Nash Bill Nash 11/6/2017

Print/Type Signature Date

Division of Enterprise Technology-Bureau of Security

Chief Information Security Officer